Negligible Events, Game Transformation and Formal Proofs of Cryptographic Protocols

Jesús Almansa Tatsuaki Okamoto

NTT Labs
Information Sharing Platform

1st JSIAM - FAIS Workshop
University of Tokyo
July 26, 2006

motivation

Consider a typical security definition in the attack-based approach:

1. $\mathtt{Game}^0 \stackrel{\mathtt{def}}{=} [\, x_1 \stackrel{¢}{\leftarrow} A^1, x_2 \stackrel{¢}{\leftarrow} A^2(x_1), \ldots, x_n \stackrel{¢}{\leftarrow} A(x_1, \ldots, x_{n-1}) \,]_k$

2. $\mathtt{ADV}^0_A(k) \stackrel{\mathtt{def}}{=} P[x_n = x_i]$ (x_i not an input of A)

3. Security: $|\mathtt{ADV}^0_A(k) - r|$ is negligible as a function of k $(*)$

Here,

- A_i, A are PPT algorithms or finite sets
- $x_i \stackrel{¢}{\leftarrow} A_i(x_1, \ldots, x_{i-1})$ represents the assignment to x_i of a value sampled at random from the distribution ¢ of A_i wrt values of (some among) $x_1, \ldots, x_{i-1}$.

To prove $(*)$, one provides a “slightly modified” game ...

motivation

1. $\mathtt{Game}^1 \stackrel{\mathtt{def}}{=} [\ y_1 \stackrel{¢}{\leftarrow} B^1, y_2 \stackrel{¢}{\leftarrow} B^2(y_1), \ldots, y_n \stackrel{¢}{\leftarrow} A(y_1, \ldots, y_{n-1})\ ]_k$

2. $\mathtt{ADV}^1_A(k) \stackrel{\mathtt{def}}{=} P[y_n = y_j]$ (y_j not an input of A)

... and one shows that

a. $|\mathtt{ADV}^0_A(k) - \mathtt{ADV}^1_A(k)|$ is negligible as a function of k

b. $|\mathtt{ADV}^1_A(k) - r|$ is negligible as a function of k

Rationale:
if $\mathtt{ADV}^0_A(k)$ and $\mathtt{ADV}^1_A(k)$ are "close", and $\mathtt{ADV}^1_A(k)$ is "close to r", then $\mathtt{ADV}^0_A(k)$ is "close to r".

Intuition: $\mathtt{Game}^0$ and $\mathtt{Game}^1$ have "similar structures", but the latter is easier to analyse.

motivation

This is the *game-transformation* technique for proving security of crypto protocols. [Shoup,Bellare-Rogaway,GGM]
Benefits:

- simplicity (understanding)
- proof pattern (just like Modus Ponens is)
- rigorous (mathematical language)
- exact bounds (security bounds)
- practical (extensively used)
- automation (computer aid) [Blanchet-Pointcheval]

By no means it is the final solution to proofs of crypto protocols!
It is just that its benefits are too important.

motivation

However: The attack-based approach is just one paradigm among other definitional paradigms for crypto security.

In particular, *simulation-based* approaches fit better to study concurrent multiparty protocols: PCL, PIOA, PPT, RS, UC.

- no *explicit* proof technique for simulation-based approaches *with same benefits* of game-transformation technique. (except maybe for [PIOA])

Our aim: apply the game-transformation proof technique in simulation-based approaches.

agenda

abstraction

reality

formality

abstraction

abstraction

In technical terms, the elements we deal with are

- a probability space family
  $[\![\{(\Omega_k, P_k)\}_{k\in\mathbb{N}}]\!] = \{\mathtt{Game}_k\}_{k\in\mathbb{N}}$
- a random ensemble
  $[\![\{X_k\}_{k\in\mathbb{N}}]\!] = \{\mathtt{ADV}_A(k)\}_{k\in\mathbb{N}}$

And the problem we want to solve is:

Is there a “natural” way h of transforming $\{(\Omega_k, P_k)\}_{k\in\mathbb{N}}$
s.t. $\{X_k\}_{k\in\mathbb{N}} \approx h(\{X_k\}_{k\in\mathbb{N}})$
(possibly under certain extra assumptions)

Answer: Yes!

abstraction

Given a psf $\{(\Omega_k, P_k)\}_{k\in\mathbb{N}}$, an event ensemble is a sequence $X = \{X_k\}_{k\in\mathbb{N}}$, where X_k is a boolean random variable on Ω_k for each k.

- $X_k : \Omega_k \to \{0, 1\}$
- $X_k = 1$ is an event of Ω_k.

To each $X = \{X_k\}_{k\in\mathbb{N}}$ there corresponds a function $F^X : k \mapsto P_k[X_k = 1]$.

Def. Let $\Omega = \{(\Omega_k, P_k)\}_{k\in\mathbb{N}}$ be a psf. Let $r \in [0, 1]$.

1. X is r-negligible iff F^X is negligibly close to r.
2. $\mathfrak{N}_r$ is the collection of all r-negligible ensembles.
3. $\mathfrak{N} = \cup_r \mathfrak{N}_r$

abstraction

For instance, $\mathbf{0} \in \mathfrak{N}_0$ and $\mathbf{1} \in \mathfrak{N}_1$.

In principle, there is an uncountable number of $\mathfrak{N}_r$'s; but in reality many of them will be empty.

A natural way of relating ensembles:
Def. Let $\Omega = \{(\Omega_k, P_k)\}_{k\in\mathbb{N}}$ be a psf. We write $X \overset{s}{\approx} Y$, and say that X is statistically indistinguishable to Y iff F^X is negligibly close to F^Y.

Some properties:

- $\overset{s}{\approx}$ is an equivalence relation.
- $\mathfrak{N}_r$ is a class modulo $\overset{s}{\approx}$, for any $r \in [0,1]$.
- If $X\overline{Y} \overset{s}{\approx} 0$ and $Y \in \mathfrak{N}_0$ then $X \in \mathfrak{N}_0$.
- Shoup's Difference Lemma:
  If $X\overline{Z} \overset{s}{\approx} Y\overline{Z}$ and $Z \in \mathfrak{N}_0$, then $X \overset{s}{\approx} Y$.

abstraction

So far we have focused on a single psf. However, we are trying to explain how to transform a psf into another that is structurally close.

Def. Consider $\langle \Omega, \mathfrak{N} \rangle$ and $\langle \Omega', \mathfrak{N}' \rangle$. A morphism is a transformation $h = \{h_k\}_{k \in \mathbb{N}}$ such that

- $h_k : \Omega_k \to \Omega'_k$;
- $h^{-1}(N) \in \mathfrak{N}$ for all $N \in \mathfrak{N}'$.

This is what we are looking for!

Assume $\langle \Omega, \mathfrak{N} \rangle$ is given and let X be an ensemble for Ω. If there exists a morphism h into $\langle \Omega', \mathfrak{N}' \rangle$ such that $h(X) \in \mathfrak{N}'$, then $X \in \mathfrak{N}$.

reality

reality

A model for our theory is anything that gives rise to well-defined psf's.

E.g., a specification/programming language to describe/define interaction of PPT entities, with a well defined *probabilistic semantics*.

What could we prove?

- unconditional security in both attack-based and simulation-based approach via game transformation.
- computational security in attack-based approach via *direct* arguments

reality

Study case: ElGamal encryption

1. $$\left[\begin{array}{l} x \xleftarrow{\mathtt{u}} \mathbb{Z}_q,\ \alpha \leftarrow \gamma^x \\ (m_0, m_1) \xleftarrow{¢} A(\alpha), \\ b \xleftarrow{\mathtt{u}} \{0,1\} \\ y \xleftarrow{\mathtt{u}} \mathbb{Z}_q,\ \beta \leftarrow \gamma^y,\ \delta \leftarrow \alpha^y,\ \zeta \leftarrow \delta \cdot m_b \\ \hat{b} \xleftarrow{¢} A(\alpha, \beta, \zeta) \end{array}\right]$$
2. $\mathtt{ADV}_A(k) = |P[b = \hat{b}] - 1/2|$
3. Security: $\mathtt{ADV}_A(k)$ is negligible, as a function of k, for all PPT A.

Security of ElGamal encryption is claimed to hold under the Decisional Diffie-Hellman assumption (DDH)

reality

Decisional Diffie-Hellman

1.
$$
\begin{array}{l}
[\quad x \stackrel{\mathtt{u}}{\leftarrow} \mathbb{Z}_q,\ \alpha \leftarrow \gamma^x \\
\quad y \stackrel{\mathtt{u}}{\leftarrow} \mathbb{Z}_q,\ \beta \leftarrow \gamma^y, \\
\quad z \stackrel{\mathtt{u}}{\leftarrow} \mathbb{Z}_q \\
\quad d \stackrel{\mathtt{u}}{\leftarrow} \{0,1\} \\
\quad \delta \leftarrow \begin{cases} \alpha^y & \text{, if } d = 0 \\ \gamma^z & \text{, if } d = 1 \end{cases} \\
\quad \hat{d} \stackrel{\text{¢}}{\leftarrow} D(\alpha, \beta, \delta) \qquad\qquad]
\end{array}
$$

2. $\mathtt{ADV}_D(k) = |P[d = \hat{d}] - 1/2|$
3. DDH: $\mathtt{ADV}_D(k)$ is negligible, as a function of k, for all PPT D.

reality

We could play them both at once:

$$
\begin{aligned}
[\quad & x \xleftarrow{u} \mathbb{Z}_q,\ \alpha \leftarrow \gamma^x \\
& (m_0, m_1) \xleftarrow{¢} A(\alpha), \\
& b \xleftarrow{u} \{0,1\} \\
& y \xleftarrow{u} \mathbb{Z}_q,\ \beta \leftarrow \gamma^y, \\
& z \xleftarrow{u} \mathbb{Z}_q \\
& d \xleftarrow{u} \{0,1\} \\
& \delta \leftarrow \begin{cases} \alpha^y & \text{, if } d = 0 \\ \gamma^z & \text{, if } d = 1 \end{cases} \\
& \zeta \leftarrow \delta \cdot m_b \\
& \hat{d} \xleftarrow{¢} D(\alpha, \beta, \delta) \\
& \hat{b} \xleftarrow{¢} A(\alpha, \beta, \zeta) \qquad\qquad]
\end{aligned}
$$

$$Y_k = \mathtt{ADV}_D(k) = |P[d = \hat{d}] - 1/2|$$

$$X_k = \mathtt{ADV}_A(k) = |P[d = 0 \wedge b = \hat{b}] - 1/2|$$

reality

$$Y_k = \mathtt{ADV}_D(k) = |P[d = \hat{d}] - 1/2|$$
$$X_k = \mathtt{ADV}_A(k) = |P[d = 0 \wedge b = \hat{b}] - 1/2|$$

Consider then $X = \{X_k\}_{k \in \mathbb{N}}$ and $Y = \{Y_k\}_{k \in \mathbb{N}}$.
Under the assumption that $Y \in \mathfrak{N}_0$, then $X \in \mathfrak{N}_0$.

Indeed, we know that
$X\overline{Y} \overset{s}{\approx} 0$, and $Y \in \mathfrak{N}_r$ implies $X \in \mathfrak{N}_r$.

formality

formality

"formal" can mean several things:

- serious
- official
- precise
- methodical
- form over contents

does our theory allow us to argue formally
(in the above sense)?
yes! it is already a gain vs common practice.

could we actually automate our proofs? possibly...

formality

once determined the ensemble on which a property is to be proved, the reasoning is symbolic.

- *boolean* ensembles inherit algebra of sets
- with $=$, the same axioms of algebra of sets apply
- with $\stackrel{s}{\approx}$, some more axioms are added, some more inference rules are added
- the type of probability spaces we use in practice (discrete product spaces) seem to provide some natural subevent relation
- applying game transformation is more challenging; not easy to decide in fully automated fashion what transformation to apply among many other
- guaranteeing computational security using game transformation requires more effort.

ALGEBRA OF ENSEMBLES WRT $=$

Commutative:	$XY = YX$	$X + Y = Y + X$
Associative:	$X(YZ) = (XY)Z$	$X + (Y + Z) = (X + Y) + Z$
Distributive:	$X(Y + Z) = XY + XZ$	$X + YZ = (X + Y)(X + Z)$
Tautology:	$XX = X$	$X + X = X$
Absorption:	$X(X + Y) = X$	$X + XY = X$
Complementation:	$X\overline{X} = 0$	$X + \overline{X} = 1$
Double Complementation:	$\overline{\overline{X}} = X$	
De Morgan:	$\overline{XY} = \overline{X} + \overline{Y}$	$\overline{X + Y} = \overline{X}\,\overline{Y}$
Neutrals:	$0X = 0$	$1 + X = 1$
	$1X = X$	$0 + X = X$
	$\overline{0} = 1$	$\overline{1} = 0$

Thank you.